UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

IN RE: CHANGE HEALTHCARE, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 24-md-03108 (DWF/DJF)
This Document Relates to All Actions	**JOINT STATEMENT REGARDING THE PROPOSED ELECTRONICALLY STORED INFORMATION PROTOCOL, PROTECTIVE ORDER, COORDINATION ORDER, AND DISCOVERY**

Pursuant to the Court's February 19 and 28, 2025, minute orders (ECF Nos. 215, 224), the Parties submit a Proposed Order regarding the Protective Order and the Discovery of Electronically Stored Information ("ESI") to govern this Action. The Parties have exchanged drafts of a Proposed Protective Order and Proposed ESI Protocol, met and conferred numerous times, and submitted a Joint Status Report to this Court on February 18, 2025, summarizing the Parties' positions and identifying areas of impasse. The Parties have resolved all but two issues in the Protective Order and four issues in the ESI Protocol, which they hereby submit to the Court for resolution.

A Proposed Protective Order is attached as Exhibit A and a Proposed ESI Protocol is attached as Exhibit B, each reflecting the provisions agreed upon by the parties, as well as the provisions that remain disputed. The disputed issues, and the parties' respective positions on those issues, are provided below. These disputed issues are also highlighted in the corresponding exhibits. Plaintiffs' proposed language is highlighted in yellow, and

Defendants' proposed language is highlighted in turquoise.

PROPOSED PROTECTIVE ORDER

There are two disputed provisions, which are found in three separate paragraphs of the proposed Protective Order. The first issue, which is in paragraph 12(f), relates to whether there should be any "presumptively privileged" documents. The second issue, addressed in paragraphs 14 and 15, relates to whether documents designated as Confidential or Highly Confidential can be shown to affiliates of the Producing or Designating party.

Plaintiffs' Position:

¶ 12(f) - Assertion of Privilege:

The Parties have reached impasse on whether there should be "presumptively privileged" categories of documents, which therefore can be unilaterally not included on a privilege log. Initially, Plaintiffs proposed a more narrow scope for the presumption, starting at the time of the first-filed complaint and limiting it to documents specifically related to legal advice from counsel and attorney work product. Parties could not reach agreement on such a limitation.

The Federal Rules of Civil Procedure make clear that any party withholding documents on the basis of privilege must provide certain information to a requesting party. Plaintiffs therefore believe that there should not be broad categories exempt from the rule on privilege logs and that the Parties should instead follow Fed. R. Civ. P. 26. Under this Rule, a party who withholds information that is otherwise discoverable on the grounds of privilege is required to "describe the nature of the documents,

communications or tangible things not produced or disclosed" and to do so by putting those documents on the privilege log. Fed. R. Civ. P. 26. Because the Parties cannot agree on limitations of a "presumptively privileged" provision, Plaintiffs believe that the default provided by the Federal Rules of Civil Procedure is appropriate.

Defendants cite to a number of protective orders to support their argument that this provision, as written by Defendants, is standard in many data breach class actions and MDLs. While some of these protective orders include provisions similar to Defendants' proposal, not all do. For instance, the provision Defendants cite to from *In re: MOVEit Customer Data Sec. Breach Litig.* states that a party is not required to include on a privilege log any "document written, created, or drafted by, or communications with, *outside counsel* after the date of the *filing of the first complaint naming that party.*" *In re: MOVEit Customer Data Sec. Breach Litig.*, No. 1:23-md-03083, ECF No. 912 (D. Mass. May 28, 2024), at ¶ 41 (emphasis added). Plaintiffs proposed similar language in this Action, but Defendants rejected limiting the presumptively privileged provision to documents and communications after the date of the first filed complaint. This is demonstrative that while it may not be uncommon to include a provision to exempt presumptively privileged communications, the language proposed by Defendants ought not to be considered "standard".

Put shortly, the language proposed by Defendants is simply too broad. As written, it will encompass any document that touches on the issues related to the Data Breach. Without such documents included on the privilege log, Plaintiffs will have no opportunity to challenge the designation. This is particularly problematic because the presumption as

written will apply to documents related to forensic investigations undertaken by agents of Defendant corporate entities. This is an issue already teed up for dispute, and Defendants' sweeping proposal will hide these critical documents from analysis.

¶¶ 14(k) and 15(a) and (b) - Disclosure of Confidential or Highly Confidential Discovery Material

These paragraphs identify who can see Discovery Materials that are marked Confidential or Highly Confidential. The disagreements are found in the categories relating to whether disclosures of documents marked Confidential or Highly Confidential can be made to corporate "affiliates" of the Producing or Designating Party. Given that there are multiple Defendants in this case who are members of the same corporate families (i.e. affiliates), Plaintiffs believe that it is reasonable that documents from one member of that corporate family should be available to show to another member of the corporate family regardless of the Confidential designation. The purpose of these designations is to prevent disclosure of documents containing confidential information to a potential competitor (or other party who may use that information either to benefit themselves or harm the Designating Party). But here, because the corporate affiliates are all part of the same corporate family, that concern does not exist. Limiting the ability to use documents across corporate families, especially in this case where conduct at issue crosses between entities within the corporate family, will prevent Plaintiffs from effectively deposing witnesses on issues that affect or are across the affiliated corporate Defendants. Without this language, Plaintiffs would be prevented (for example) from using relevant documents with a Change Healthcare executive about a Temporary Funding Assistance Program (TFAP) loan

because a Provider Plaintiff contracted with Optum instead of Change Healthcare directly.

Defendants' Position:

¶ 12(f) - Assertion of Privilege

Plaintiffs oppose a standard provision to exempt presumptively privileged communications and work product from the Parties' privilege log obligations. This proposal is not a novel concept—it is consistent with the approach in most other data breach class actions and MDLs. *See, e.g., Crowe v. Managed Care of North America*, No. 0:23-cv-61065, ECF No. 153 (S.D. Fla. June 14, 2024), at ¶ 59; *In re: MOVEit Customer Data Sec. Breach Litig.*, No. 1:23-md-03083, ECF No. 912 (D. Mass. May 28, 2024), at ¶ 41; *In re: Marriott International Customer Data Sec. Breach Litig.*, No. 8:19-md-02879, ECF No. 781 (D. Md. Apr. 26, 2021), at ¶ 11; *In re: AMCA Customer Data Sec. Breach Litig.*, No. 2:19-md-02904, ECF No. 243 (D.N.J. Oct. 26, 2020), at ¶ 52; *In re: Anthem, Inc. Data Breach Litig.*, No. 5:15-md-02617, ECF No. 352 (N.D. Cal. Nov. 4, 2015), at ¶ 8. Nearly all of these examples tie this provision to the date the impacted entity discovered the data breach or the date it announced that data breach. Consistent with those examples, Defendants' proposed language keys this provision to February 21, 2024—the date that Defendants became aware of the Cyberattack. Notwithstanding Plaintiffs' attempt to distinguish the language accepted in *MOVEit*, which tied this provision to the date of the filing of the first complaint naming the party that is claiming privilege, that case offers Plaintiffs no support for their current position that *no* documents be considered presumptively privileged.

The practice of exempting presumptively privileged documents from privilege logs

is standard for good reason. Immediately after suffering a cyberattack, companies turn to internal and external legal counsel to assist with legal needs and to prepare for anticipated litigation. In this matter, ten cases were filed within the first month of Change Healthcare announcing it had discovered the cyberattack. Plaintiffs' insistence that the Parties must review and log an exorbitant number of documents that the Parties will undoubtedly agree are privileged is entirely unreasonable because of the unnecessary burden, cost, and time it will require—not just for Defendants, but also for the 28 Named Plaintiffs in the Provider MDL Track that were likely consulting counsel following the cyberattack, and that will have their own privilege log obligations to undertake in discovery. Despite this excessive burden, Plaintiffs have not offered any rational basis or precedent to justify why the Parties should log these communications.

¶¶ 14(k) and 15(a) and (b) – Disclosure of Confidential or Highly Confidential Discovery Material

Plaintiffs insist on including a blanket permission for disclosure of confidential and highly confidential discovery materials to any affiliated entity of any Producing Party, without that Producing Party's prior consent and without any restrictions or contemplated process in place. Under Plaintiffs' proposed arrangement, for example, it is permissible to disclose highly confidential material produced by one UnitedHealth Group entity, of which there are many, to any affiliated entity without UnitedHealth Group's consent, even where such affiliated entity may not be a party to this Action. Such a proposal ignores any contractual limitations, internal company policies, or court decisions that must be complied with in order for such disclosure to be acceptable. Although Defendants do not oppose

disclosures to affiliated entities pursuant to an appropriate meet-and-confer process, Plaintiffs' unrestricted approach is unworkable.

PROPOSED ESI PROTOCOL

There are four paragraphs of the proposed ESI Protocol in which the parties have disputes. The first issue, found in Section II.b, relates to language setting out the applicability of certain laws and statutes. The second issue, found in Section IV, relates to the production of structured data, specifically with reference to the database dictionary. The third issue, found in Section V.e., identifies data categories that the Parties agree are inaccessible, and therefore not discoverable, and should not be preserved. While the Parties agree on many of these provisions, there is one category in which the Parties do not agree. The last issue arises under VII.d. and relates to the issue of hyperlinks for documents with a "Parent-Child Relationship."

Plaintiffs' Positions:

Section II.b. - Applicability

Plaintiffs seek to make clear that nothing in the ESI Protocol is intended to be an exhaustive list of obligations and that the Parties must still comply with "any other applicable state of federal statutes, orders, and rules". Plaintiffs contend the inclusion of this language is particularly important as this case is likely to involve confidential medical information as well as ongoing state court cases. Plaintiffs' language ensures all protections afforded by the Health Insurance Portability and Accountability Act ("HIPAA") and provides the protection that related state court proceedings are not superseded by this Agreement. This language does not prohibit state court parties from

filing their own ESI protocols but affords the protections necessary. While the Parties continue to negotiate the Coordination Order, Plaintiffs maintain it is necessary to include references to all state statutes, orders, and rules as they will offer protection to all parties seeking to bring a claim related to this Action. While Minnesota statutes, orders, and rules may not be binding in this MDL, they are nonetheless illustrative and will act as a guidepost for other related actions seeking to litigate this case efficiently.

Section IV - Production of Structured Data

The key distinction between the two proposals is Plaintiffs' proposed language surrounding a database dictionary. Such a tool allows the requesting Party to understand the nature and function of the structured data source and the meaning of structured data produced. This will streamline the exchange of discovery. Defendants' position that this inclusion is premature is perplexing. This Protocol is intended to govern all productions throughout the entirety of this Action, so now is the appropriate time to raise this issue.

Section V.e. - Non-Discoverable Information

This paragraph identifies data categories that the Parties agree are inaccessible, and therefore not discoverable, and should not be preserved. Plaintiffs have agreed to many of these categories but disagree with Defendants' inclusion of "data remaining on servers that have been quarantined or decommissioned for the security of the systems and/or networks". In Plaintiffs' view these are not inaccessible documents. The fact that some servers have been quarantined or decommissioned for security could likely encompass the very servers or networks at issue in this case. This language is too broad and should be rejected. Contrary to Defendants' assertion, Plaintiffs do not want

Defendants to endanger their systems as part of the discovery process. Rather, Plaintiffs want to find a safe way to access the data on quarantined or decommissioned servers as the very documents at issue are likely to be on those servers.

VII.d. - Parent-Child Relationships.

Plaintiffs have proposed the requirement that any part of a responsive email, including hyperlinks, be produced. Defendants contend that inclusion of hyperlinks could be overly burdensome. That, however, is a concern raised only in the abstract. Perhaps there will be some instances that may raise concerns but a bright line rule excluding all this information is too harsh and too speculative. It is also unclear how this can be overly burdensome. It is Plaintiffs' understanding that with the correct email system and license, the hyperlink files can typically be retrieved. A complete exclusion of the language pertaining to hyperlinks is extreme and could lead to discoverable and relevant information being excluded without a reasonable basis.

Furthermore, technological advancements have led to the use of more links and cloud-based systems, as opposed to attachments. These "technological advancements cannot and should not be used to circumvent or obstruct discovery. Nor should parties be permitted to simply throw their hands up at the technical impositions of producing discovery from cloud-based systems." Lea Malani Bays, *The Missing Links: Why Hyperlinks Must Be Treated as Attachments in Electronic Discovery*, 92 U. Cin. L. Rev. 979 (2024). Given that the use of hyperlinks are becoming more of the norm, as opposed to an exception, it is unreasonable to exclude the production of hyperlinks in responsive emails.

Defendants' Positions:

Section II.b. - Applicability

To the extent Plaintiffs seek to include protections for data covered by HIPAA, that is adequately addressed in the Protective Order, which is a Qualified HIPAA Protective Order, and is unnecessarily duplicative to include in the ESI Protocol. References to state laws in the MDL ESI Protocol are inappropriate because the MDL court cannot bind state courts (and vice versa), and the inclusion of these generic references could cause unintended consequences for the MDL parties. Defendants instead suggest that the parties to each state court matter negotiate an ESI Protocol that closely mirrors the final MDL ESI Protocol. This arrangement would clearly delineate which matters are subject to federal rules and statutes, and which matters are subject to state rules and statutes.

Section IV - Production of Structured Data

Plaintiffs' proposal for a mandatory production of a data dictionary in every instance regardless of burden or other considerations is premature at this time. Indeed, it is not yet known if this information exists for all databases and other structured data that will be produced. Particularly if databases have been segregated, discontinued or migrated, it might not be feasible to provide all of the information that Plaintiffs' language demands. It is unnecessary to set a mandatory requirement now, when Defendants have proposed that the Parties meet and confer concerning each database to discuss the particular production format and necessary materials to understand the same.

Section V.e. - Non-Discoverable Information:

Defendants' quarantined servers, and the data on them, were quarantined after the cyberattack for a reason—to isolate those systems and any malicious software on those systems in order to secure Change's network. Defendants have attempted to compromise on this issue by including the phrase "and where there is no reasonable way to retrieve the data without compromising the security of the systems and/or network." By rejecting this proposal, Plaintiffs appear to suggest that they are entitled to these materials even if their requests could compromises the security of Defendants' systems/network. While Defendants are willing to meet and confer in good faith on how to access these potentially dangerous materials, no Party should be forced to endanger their systems as part of the discovery process.

VII.d. - Parent-Child Relationships

The collection of hyperlinked materials is not appropriate for several reasons. First, the linked material content is not actually present in the email or attachment at issue. Second, unlike email attachments, hyperlinked materials can—and frequently do—change between the time the hyperlink is generated and when the hyperlinked material is collected. Third, the production of hyperlinked materials from emails or attachments is very burdensome and often impossible using Defendants' current email archive system. This is not an abstract concern, but one raised after investigating the particular archive system currently in use by Defendants. The blanket production of hyperlinked materials is not standard, especially in situations such as this one where the technical specifications of an archive system make such production exceptionally burdensome. See, e.g., *Crowe v. Managed Care of North America*, No. 0:23-cv-61065, ECF No. 153 (S.D. Fla. June 14,

2024), at ¶ 35; *In re: MOVEit Customer Data Sec. Breach Litig.*, No. 1:23-md-03083, ECF No. 911 (D. Mass. May 28, 2024), at ¶ 30; *In re: AMCA Customer Data Sec. Breach Litig.*, No. 2:19-md-02904, ECF No. 243 (D.N.J. Oct. 26, 2020), at ¶ 24.

PROPOSED COORDINATION ORDER

The Parties have agreed on a Proposed Coordination Order, which is attached as Exhibit C.

EARLY DISCOVERY

After numerous email exchanges and meet and confers, the parties have made significant progress concerning the exchange of early discovery. Each party has agreed to produce specific reasonably-accessible non-privileged documents that can be collected without email searches, forensic collection, or other ESI methods of collection. The parties also reserve all rights as to formal objections under Rule 34 as to scope, relevance, and any other objection permitted under the Rules.

The Parties' Agreements regarding Early Discovery: Named plaintiffs in the Patient Track have agreed to produce the following categories of documents:

1. Documents relating to injuries, harms, risks, losses, or damages that named Plaintiffs suffered as a result of the Data Breach.
2. Documents relating to measures Plaintiffs took to monitor, mitigate, or protect against their injuries, risks, harms, losses, or damages.
3. Documents relating to notices Plaintiffs received from any Defendant(s) or other sources indicating that Plaintiffs' Personal Information may have been impacted in the Data Breach.

4. Documents relating to identity protection, identity repair, identity monitoring, credit protection, credit repair, credit monitoring, or fraud consultation services that Plaintiffs acquired, used, or obtained as a result of the Data Breach.
5. Documents relating to reimbursements Plaintiffs sought or received for any alleged or actual out-of-pocket costs Plaintiffs incurred as a result of the Data Breach.
6. Documents relating to the compromise of Plaintiffs' personal information in data breaches other than the Data Breach at issue here.

Named plaintiffs in the Provider Track have agreed to produce the following categories of documents:

1. Agreements and other easily obtainable documents reflecting bills for loans or lines of credit that were used or taken out because of the shutdown; bills for outside help with claims and billing incurred because of the shutdown; reports reflecting employee overtime incurred because of shutdown; reports reflecting unpaid or reduced salaries because of shutdown; reports reflecting claims denied as untimely because of the shutdown; reports reflecting any unprocessed claims because of the shutdown; and other easily obtainable documents reflecting Plaintiffs' alleged damages;
2. Agreements for substitute EDI services obtained after the shutdown;
3. Updates regarding restoration of Change's services from EHRs and Change/UHG, or associations the principal client contact has access to;

4. Bills or invoices that TFAP funds were used for, to the extent they are located in one place;
5. Contracts for EDI services with Change;
6. Profit and loss statements and/or balance sheets for FY 2023 and 2024; and
7. For Provider Plaintiffs part of the Change Healthcare Inc. Direct Contract Sub-Class and have made insurance claims related to the data breach, documents reflecting insurance policies and insurance claims.
8. For Provider Plaintiffs, a list of their Tax Identification Numbers.

Defendants have agreed to produce, identify, and/or describe the documents or information set forth below. However, Defendants' willingness to produce, identify, and/or describe these categories of discovery are subject to Defendant-specific personal jurisdictional objections.

1. Documents that were previously produced to the U.S. Department of Health and Human Services' ("HHS") Office for Civil Rights, and the States Attorneys General's Offices regarding the Data Breach;
2. Templates of the individual notice letters that were issued following the Data Breach;
3. Templates of "Temporary Funding Assistance" (TFA) agreements and any template communications sent to health care providers that received TFA funding.
4. Document sufficient to show the total dollar amount of TFA loans that were made by Defendants as of January 15, 2025, the total amounts of TFA loans

that have been repaid as of January 15, 2025, and the total amounts of TFA loans outstanding as of January 15, 2025.

5. Information regarding UHG's captive insurance.
6. Documents sufficient to show assessments of Change Healthcare's cybersecurity that were issued between October 3, 2022 and February 21, 2024 and that cover any portion of that period, as well as cybersecurity policies covering that time period;
7. Data retention policies that were in effect at the time the Data Breach was discovered;
8. Identification of the key persons who were responsible for data security at Change Healthcare as well as the key persons who worked on remediating the Data Breach;
9. Identification of the third-parties who assisted in the investigation and restoration efforts following the Data Breach;
10. All reportable data security incidents at Change Healthcare that occurred prior to the Data Breach;
11. How and when Defendants discovered or were notified about the Data Breach; and
12. A list of the governmental agencies that served Civil Investigative Demands and subpoenas to Defendants following the Data Breach and to whom they were issued.

Remaining Disputes.

There remain a few disputed categories of documents that parties have been unable to reach an agreement on at this time:

The first issue relates to information regarding how long Defendants' systems were down at the time of the data breach.

The second issue relates to exchanging information as to which systems stored data or PII/PHI.

The third issue relates to whether the Defendants that are challenging personal jurisdiction should be required to participate in early discovery before their motions to dismiss are decided (so as to avoid any claim of waiver).

The fourth issue is whether "forensic reports" or analysis that occurred after the breach are discoverable.

On these last two issues (the personal jurisdiction and forensic reports issues), the Parties have agreed to brief these issues separately pursuant to an agreed-upon schedule and, as such, those two issues are not addressed below.

Plaintiffs' Positions:

Duration of Systems' Non-Functionality During Data Breach

The Parties are at an impasse regarding the production of documents relating to the duration of Defendants' systems inaccessibility at the time of the data breach. Plaintiffs requested "documents related to any statements, analyses, evaluations, testing, or assessments of the time, on a per system basis, that Defendant's systems were non-operational or did not function fully because of the Data Breach." Defendants contend

that this is overly burdensome as it requires custodial searches and implicates attorney client privilege and the attorney work product doctrine. It is unclear how this can be overly burdensome. It seems to be a simple enough task to look back into records to determine how long after the data breach, Defendants were left without the use of secure systems.

Systems Used for Storing Data, PII, or PHI

The parties disagree on exchanging information as to which systems stored data or PII/PHI, as Defendants believe this is not appropriate for early discovery and is overly burdensome. Patients served two interrogatories seeking the computer networks or systems used to process, keep, or maintain data or sensitive information. It is unclear how providing the names of these computer networks, computer systems, or locations can be overly burdensome. Logically speaking, these are the very networks that Defendants would have addressed immediately upon learning of the data breach. It does not seem Defendants would need to conduct extensive search or forensic collection to determine which systems stored the data that is central to this very litigation.

Defendants' Positions:

Documents Relating to the Duration of Defendants' System Inaccessibility

As Plaintiffs' own consolidated complaints acknowledge, Defendants' restoration of its systems was an ongoing process in which systems were restored on a rolling basis. For that reason, there is no uniform method to readily identify the restoration timeline for all systems. In order to provide a complete and accurate response to this request, Defendants would be required to engage in custodial discovery and significant

investigation. As noted above, the Parties agreed that for purposes of early discovery, the Parties will produce reasonably-accessible non-privileged documents that can be collected without email searches, forensic collection, or other ESI methods of collection. The exercise of responding to this request for purposes of early discovery is beyond the bounds of the Parties' agreement. Regardless, general information regarding system restoration is publicly available. *See* https://www.unitedhealthgroup.com/ns/changehealthcare.html.

Information Concerning Systems that Stored Data or PII/PHI

It is likewise unreasonable for Plaintiffs to request a full list of Defendants' systems that stored data or PII/PHI at this early stage of the litigation. Indeed, producing this broad swath of information would be disproportional and unduly burdensome at any point in discovery—not just early discovery—because it would require Defendants to evaluate systems that have no relevance to this litigation. Moreover, even if Plaintiffs were to narrow this request to seek information from only those systems that were potentially impacted in the Data Breach, it would still require Defendants to evaluate significant information in a way that goes beyond the scope of this early discovery stage.

Dated: March 11, 2025

/s/ Daniel E. Gustafson
Daniel E. Gustafson (#202241)
GUSTAFSON GLUEK PLLC
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dgustafson@gustafsongluek.com

Overall Lead Counsel

/s/ Allison M. Ryan
Allison M. Ryan
Alicia J. Paller (#0397780)
HOGAN LOVELLS US LLP
555 13th Street NW
Washington, D.C. 20004
T. (202) 637-5600
F. (202) 637-5910
allison.holt-ryan@hoganlovells.com
alicia.paller@hoganlovells.com

Vassi Iliadis
HOGAN LOVELLS US LLP
1999 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
T. (310) 785 4600
F. (310) 785-4601
vassi.iliadis@hoganlovells.com

Counsel for Defendants